Solutions to Homework 9

1. Show that \( \mathbb{Z}_2[x]/(x^3 + x + 1) \cong \mathbb{Z}_2[y]/(y^3 + y^2 + 1) \).

**Solution:** Consider the map \( \varphi: \mathbb{Z}_2[x] \rightarrow \mathbb{Z}_2[y]/(y^3 + y^2 + 1) \) given by \( x \mapsto y+1 \), that is, \( \varphi(f) = f(y+1) \). Then \( \varphi(x^3 + x + 1) = y^3 + y^2 + 1 = 0 \), so \( (x^3 + x + 1) \subseteq \text{ker} \varphi \). But \( x^3 + x + 1 \) is irreducible, and \( \mathbb{Z}_2[x] \) is a principal ideal domain, so irreducible implies prime, and every non-zero prime ideal is maximal; hence either \( \text{ker} \varphi = (x^3 + x + 1) \) or \( \text{ker} \varphi = (1) \). Since \( \varphi(1) \neq 0 \), we must have \( \text{ker} \varphi = (x^3 + x + 1) \). Thus we get an isomorphism

\[

\mathbb{Z}_2[x]/(x^3 + x + 1) \cong \text{im} \varphi \subseteq \mathbb{Z}_2[y]/(y^3 + y^2 + 1).

\]

Since both sides have 8 elements, the inclusion must be an equality.

2. List all the irreducible polynomials of degree 4 in \( \mathbb{Z}_2[x] \).

**Solution:** A polynomial of degree 4 is either irreducible, or it factors as a linear times a cubic, or it factors as a product of two irreducible quadratics. First we list the sixteen polynomials of degree 4. We cross off the ones with no constant term, since they are multiples of \( x \). We cross off the ones with an even number of terms, since they have \( f(1) = 0 \), hence are multiples of \( (x + 1) \). This leaves us with four:

\[

x^4 + x + 1 \quad x^4 + x^2 + 1

x^4 + x^3 + 1 \quad x^4 + x^3 + x^2 + x + 1.

\]

In lecture we saw that the only irreducible quadratic is \( x^2 + x + 1 \), so we cross out \( (x^2 + x + 1)^2 = x^4 + x^2 + 1 \), leaving three irreducibles:

\[

x^4 + x + 1 \quad x^4 + x^3 + 1 \quad x^4 + x^3 + x^2 + x + 1.

\]
3. Show that \( f = x^4 + 3x^3 + 5x^2 + 7x + 9 \) is irreducible in \( \mathbb{Q}[x] \).

**Solution:** Suppose on the contrary that there are non-constant polynomials \( g, h \in \mathbb{Q}[x] \) with \( f = gh \). By Gauss's lemma there is an \( a \in \mathbb{Q} \) such that \( ag \in \mathbb{Z}[x] \) and \( a^{-1}h \in \mathbb{Z}[x] \). Let \( G = ag \) and \( H = a^{-1}h \), so \( f = GH \). Reduce mod 2, so we get \( \bar{f} = \bar{G}\bar{H} \in \mathbb{Z}_2[x] \). Since the leading coefficient of \( f \) is 1, the leading coefficients of \( G \) and \( H \) must be \( \pm 1 \), so \( \bar{G} \) and \( \bar{H} \) are again non-constant, so \( \bar{f} \) is reducible in \( \mathbb{Z}_2[x] \). But \( \bar{f} = x^4 + x^3 + x^2 + x + 1 \), and in the previous problem we saw that this is irreducible.

4. Let \( f \in \mathbb{Z}[x] \), and suppose that \( f\left(\frac{1}{2}\right) = 0 \). Show that \( 2x - 1 \mid f \).

**Solution:** See exam solutions.

5. We have seen that \( R = \mathbb{Z}[\sqrt{-5}] \) is not a unique factorization domain, much less a principal ideal domain. Show nonetheless that every non-zero prime ideal in \( R \) is maximal.

**Solution:** If \( I \) is prime then \( R/I \) is an integral domain. Below I will argue that \( R/I \) is finite. By homework 2, problem 3c, every finite integral domain is a field. Thus \( I \) is maximal.

Proposition: For any non-zero ideal \( I \subset R \), the quotient \( R/I \) is finite.

First I claim that \( I \cap \mathbb{Z} \neq (0) \). Indeed, choose a non-zero \( a + b\sqrt{-5} \); then
\[
N := (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \in I \cap \mathbb{Z}.
\]

Next I claim that \( R/(N) \) is finite, with exactly \( N^2 \) elements. Indeed, we see that \( a + b\sqrt{-5} \equiv c + d\sqrt{-5} \) (mod \( N \)) in \( R \) if and only if \( a \equiv c \) and \( b \equiv d \) (mod \( N \)) in \( \mathbb{Z} \). Thus every element of \( R \) is equivalent to exactly one element of the form \( a + b\sqrt{-5} \) with \( 0 \leq a, b < N \), and there are \( N^2 \) of these.

Last I claim that \( R/I \) is finite. Consider the map \( \varphi: R/(N) \to R/I \) defined by \( \varphi(r + (N)) = r + I \). This is well-defined because \( (N) \subset I \), so if \( r + (N) = s + (N) \) then \( r - s \in (N) \subset I \), so \( r + I = s + I \). And \( \varphi \) is clearly surjective. Because \( R/(N) \) is finite and it surjects onto \( R/I \), we see that \( R/I \) is finite.

(In fact \( \varphi \) is a homomorphism, but we don’t need this. Note that \( R/I \) is not a subset of \( R/(N) \) in any natural way.)
6. We define the field of formal Laurent series \( \mathbb{Q}((x)) \), which is like the ring of formal power series \( \mathbb{Q}[[x]] \) but we allow finitely many negative exponents:

\[
\mathbb{Q}((x)) = \{ a_{-n}x^{-n} + \cdots + a_{-1}x^{-1} + a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots \}.
\]

Let’s take for granted that \( \mathbb{Q}((x)) \) is a ring. Show that every non-zero element has an inverse, so \( \mathbb{Q}((x)) \) is a field. Show that the field of fractions of \( \mathbb{Q}[[x]] \) is isomorphic to \( \mathbb{Q}((x)) \).

Solution: First we should argue that an element

\[
a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{Q}[[x]]
\]

is a unit if \( a_0 \neq 0 \). For details of this see the exam solutions. Note that this was also homework 2, problem 4c.

Now for an arbitrary non-zero \( f \in \mathbb{Q}((x)) \), write

\[
f = a_nx^n + a_{n+1}x^{n+1} + a_{n+2}x^{n+2} + \cdots
\]

with \( a_n \neq 0 \) and \( n \) possibly negative. Factor this as

\[
f = x^n \cdot (a_n + a_{n+1}x + a_{n+2}x^2 + \cdots).
\]

The second factor is invertible in \( \mathbb{Q}[[x]] \); write

\[(a_n + a_{n+1}x + a_{n+2}x^2 + \cdots)^{-1} = b_0 + b_1x + b_2x^2 + \cdots\]

for suitable \( b_i \in \mathbb{Q} \). Then

\[
f^{-1} = x^{-n} \cdot (b_0 + b_1x + b_2x^2 + \cdots) = b_0x^{-n} + b_1x^{-n+1} + b_2x^{-n+2} + \cdots.
\]

Thus \( \mathbb{Q}((x)) \) is a field.

It remains to produce an isomorphism \( \varphi: F \to \mathbb{Q}((x)) \), where \( F \) is the field of fractions of \( \mathbb{Q}[[x]] \). Given an arbitrary \( a \in F \), write \( a = f/g \) with \( f, g \in \mathbb{Q}[[x]] \) with \( g \neq 0 \). Then \( g \) is invertible in \( \mathbb{Q}((x)) \) as we just saw, so let \( \varphi(a) = fg^{-1} \in \mathbb{Q}((x)) \). It is straightforward to check that \( \varphi \) is a well-defined homomorphism. Since \( F \) is a field, its only ideals are \((0)\) and \((1)\); since \( \varphi(1) \neq 0 \), we must have \( \ker \varphi = (0) \), so \( \varphi \) is injective. To see that \( \varphi \) is surjective, let

\[
h = a_nx^n + \cdots \in \mathbb{Q}((x))
\]

be given. If \( n \geq 0 \) then \( h \in \mathbb{Q}[[x]] \), and \( \varphi\left(\frac{1}{x^n}\right) = h \). If \( n < 0 \) then \( h^{-1} \in \mathbb{Q}[[x]] \), and \( \varphi\left(\frac{1}{x^n}\right) = h \).